MULTIMEDIA UNIVERSITY

STUDENT ID NO

TABLE NO: _____

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2019/2020

TSN3251 COMPUTER SECURITY

(All sections/groups)

10 MARCH 2020
9.00 a. m. – 11.00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of seventeen (17) printed pages only including the cover page, blank answer pages and appendix.
2. There are four (4) questions in this paper.
3. Answer ALL QUESTIONS.
4. All questions carry equal marks (25 marks) and the distribution of the marks for each sub-question is given.
5. Please write all your answers in the spaces provided in this question paper.

Question	Mark
1	
2	
3	
4	
Total	

Question 1

a) Explain the three key objectives at the heart of computer security and for each objective give an example of its application.

[9 marks]

b) Explain what a shift cipher is and what its vulnerabilities are.

[6 marks]

Continued...

c) Explain how can frequency analysis be used to conduct cryptanalysis and which type of ciphers are vulnerable?

[4 marks]

d) Bob decides to use two (2) substitution tables in his made-up encryption cipher based on the position of plaintext input characters. The two tables are as shown below.

Table for Odd Positions

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	d	g	j	m	p	s	v	y	b	e	h	k	n	q	t	w	z	c	f	i	l	o	r	u	x

Table for Even Positions

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	s	x	c	h	m	r	w	b	g	l	q	v	a	f	k	p	u	z	e	j	o	t	y	d	i

Explain how his approach affects cryptanalysis of the encryption used.

[4 marks]

Continued...

e) Explain why it is not effective to perform frequency analysis of ciphertext encrypted using a transpositional cipher

[2 marks]

Continued...

Question 2

a) Explain the difference between P-boxes and S-boxes in cryptography algorithms

[4 marks]

b) If given that the initial input to the DES subkey generation is a hexadecimal string of 0xABCDEF1234567890, answer the following sub-questions:

i. What controversy about DES keys emerged during its implementation?

[2 marks]

ii. Show how the first subkey is generated in DES using the appropriate reference tables (as listed in the appendix of this exam paper). Explain the step(s) individually then show your results as either binary OR hexadecimal strings

[10 marks]

Continued...

c) Explain the use of the S-boxes in each round of the DES cipher

[1 marks]

d) Using the S-boxes provided in the appendix, show the results of the S-box operation if given the input to the boxes in a particular DES round is 0xFEDCBA987654

[8 marks]

Continued...

Question 3

a) What are brute-force attacks?

[4 marks]

b) Explain briefly how public key ciphers can be used to provide confidentiality and authentication in communication between two parties. What is the disadvantage of using public key encryption for this operation?

[4 marks]

Continued...

c) Explain the general steps to generate the public and private keys in the RSA cipher. In your explanation, show how these keys can be generated if given the two starting values used in the calculation are 2 and 7.

[7 marks]

d) Using the keys generated in (c) show how plaintext character "E" can be encrypted and decrypted successfully using RSA.

[4 marks]

Continued...

e) Several steps can be taken to ensure RSA is implemented properly. Briefly state and describe any 3 (three) of the steps.

[6 marks]

Continued...

Question 4

a) Three (3) classic error types that have enabled many security breaches are (i) Buffer Overflows, (ii) Incomplete Mediation, and (iii) Time-of-Check to Time-of-Use Errors.
Explain each of the three (3) types mentioned above and also state how they can be prevented or mitigated

[6 marks]

Continued...

b) There are many concerns for security in a network. One of them is because of "*sharing*". In sharing the resource and workload of networks, more users have the potential to access networked systems than single computers. State and explain at least another THREE (3) issues of network security?

[6 marks]

Continued...

c) Briefly describe any three (3) out of the seven issues that are addressed by a security plan.

[6 marks]

Continued...

d) What are the advantages and disadvantages of using biometric methods for authentication (give two for each)

[4 marks]

e) Explain how SMURF attacks result in denial-of-service events.

[3 marks]

End of paper

This page is intentionally left blank for you to use as additional space for your answers. Please write the (sub)question number clearly for any answers written here

This page is intentionally left blank for you to use as additional space for your answers. Please write the (sub)question number clearly for any answers written here

APPENDIX
DES reference tables

Input message tables

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(c) Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Subkey tables

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	
3	28	15	6	21	10	
23	19	12	4	26	8	
16	7	27	20	13	2	
41	52	31	37	47	55	
30	40	51	45	33	48	
44	49	39	56	34	53	
46	42	50	36	29	32	

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1